THE WHITE HOUSE

WASHINGTON

September 17, 1984

National Security
Decision Directive 145
(Unclassified Version)

NATIONAL POLICY ON TELECOMMUNICATIONS AND AUTOMATED INFORMATION SYSTEMS SECURITY

Recent advances in microelectronics technology have stimulated an unprecedented growth in the supply of telecommunications and information processing services within the government and throughout the private sector. As new technologies have been applied, traditional distinctions between telecommunications and automated information systems have begun to disappear. Although this trend promises greatly improved efficiency and effectiveness, it also poses significant security challenges. Telecommunications and automated information processing systems are highly susceptible to interception, unauthorized electronic access, and related forms of technical exploitation, as well as other dimensions of the hostile intelligence threat. The technology to exploit these electronic systems is widespread and is used extensively by foreign nations and can be employed, as well, by terrorist groups and criminal elements. Government systems as well as those which process the private or proprietary information of US persons and businesses can become targets for foreign exploitation.

Within the government these systems process and communicate classified national security information and other sensitive information concerning the vital interests of the United States. Such information, even if unclassified in isolation, often can reveal highly classified and other sensitive information when taken in aggregate. The compromise of this information, especially to hostile intelligence services, does serious damage to the United States and its national security interests. A comprehensive and coordinated approach must be taken to protect the government's telecommunications and automated information systems against current and projected threats. This approach must include mechanisms for formulating policy, for overseeing systems security resources programs, and for coordinating and executing technical activities.

This Directive: Provides initial objectives, policies, and an organizational structure to guide the conduct of national activities directed toward safeguarding systems which process or communicate sensitive information from hostile exploitation; establishes a mechanism for policy development; and assigns

responsibilities for implementation. It is intended to assure full participation and cooperation among the various existing centers of technical expertise throughout the Executive Branch, to promote a coherent and coordinated defense against the hostile intelligence threat to these systems, and to foster an appropriate partnership between government and the private sector in attaining these goals. This Directive specifically recognizes the special requirements for protection of intelligence sources and methods. It is intended that the mechanisms established by this Directive will initially focus on those automated information systems which are connected to telecommunications transmission systems.

1. Objectives. Security is a vital element of the operational effectiveness of the national security activities of the government and of military combat readiness. Assuring the security of telecommunications and automated information systems which process and communicate classified national security information, and other sensitive government national security information, and offering assistance in the protection of certain private sector information are key national responsibilities. I, therefore, direct that the government's capabilities for securing telecommunications and automated information systems against technical exploitation threats be maintained or improved to provide for:

a. A reliable and continuing capability to assess threats and vulnerabilities, and to implement appropriate, effective countermeasures.

b. A superior technical base within the government to achieve this security, and support for a superior technical base within the private sector in areas which complement and enhance government capabilities.

c. A more effective application of government resources and encouragement of private sector security initiatives.

d. Support and enhancement of other policy objectives for national telecommunications and automated information systems.

2. Policies. In support of these objectives, the following policies are established:

a. Systems which generate, store, process, transfer or communicate classified information in electrical form shall be secured by such means as are necessary to prevent compromise or exploitation.

b. Systems handling other sensitive, but unclassified, government or government-derived information, the loss of which could adversely affect the national security interest,

shall be protected in proportion to the threat of exploitation and the associated potential damage to the national security.

c. The government shall encourage, advise, and, where appropriate, assist the private sector to: identify systems which handle sensitive non-government information, the loss of which could adversely affect the national security; determine the threat to, and vulnerability of, these systems; and formulate strategies and measures for providing protection in proportion to the threat of exploitation and the associated potential damage. Information and advice from the perspective of the private sector will be sought with respect to implementation of this policy. In cases where implementation of security measures to non-governmental systems would be in the national security interest, the private sector shall be encouraged, advised, and, where appropriate, assisted in undertaking the application of such measures.

d. Efforts and programs begun under PD-24 which support these policies shall be continued.

3. Implementation. This Directive establishes a senior level steering group; an interagency group at the operating level; an executive agent and a national manager to implement these objectives and policies.

4. Systems Security Steering Group.

a. A Systems Security Steering Group consisting of the Secretary of State, the Secretary of the Treasury, the Secretary of Defense, the Attorney General, the Director of the Office of Management and Budget, the Director of Central Intelligence, and chaired by the Assistant to the President for National Security Affairs is established. The Steering Group shall:

(1) Oversee this Directive and ensure its implementation. It shall provide guidance to the Executive Agent and through him to the National Manager with respect to the activities undertaken to implement this Directive.

(2) Monitor the activities of the operating level National Telecommunications and Information Systems Security Committee and provide guidance for its activities in accordance with the objectives and policies contained in this Directive.

(3) Review and evaluate the security status of those telecommunications and automated information systems that handle classified or sensitive government or government-derived information with respect to established objectives and priorities, and report findings and recommendations through the National Security Council to the President.

(4) Review consolidated resources program and budget proposals for telecommunications systems security, including the COMSEC Resources Program, for the US Government and provide recommendations to OMB for the normal budget review process.

(5) Review in aggregate the program and budget proposals for the security of automated information systems of the departments and agencies of the government.

(6) Review and approve matters referred to it by the Executive Agent in fulfilling the responsibilities outlined in paragraph 6. below.

(7) On matters pertaining to the protection of intelligence sources and methods be guided by the policies of the Director of Central Intelligence.

(8) Interact with the Steering Group on National Security Telecommunications to ensure that the objectives and policies of this Directive and NSDD-97, National Security Telecommunications Policy, are addressed in a coordinated manner.

(9) Recommend for Presidential approval additions or revisions to this Directive as national interests may require.

(10) Identify categories of sensitive non-government information, the loss of which could adversely affect the national security interest, and recommend steps to protect such information.

b. The National Manager for Telecommunications and Information Systems Security shall function as executive secretary to the Steering Group.

5. The National Telecommunications and Information Systems Security Committee.

a. The National Telecommunications and Information Systems Security Committee (NTISSC) is established to operate under the direction of the Steering Group to consider technical matters and develop operating policies as necessary to implement the provisions of this Directive. The Committee shall be chaired by the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) and shall be composed of a voting representative of each member of the Steering Group and of each of the following:

The Secretary of Commerce
The Secretary of Transportation
The Secretary of Energy

Chairman, Joint Chiefs of Staff
Administrator, General Services Administration
Director, Federal Bureau of Investigation
Director, Federal Emergency Management Agency
The Chief of Staff, United States Army
The Chief of Naval Operations
The Chief of Staff, United States Air Force
Commandant, United States Marine Corps
Director, Defense Intelligence Agency
Director, National Security Agency
Manager, National Communications System

b. The Committee shall:

(1) Develop such specific operating policies, objectives, and priorities as may be required to implement this Directive.

(2) Provide telecommunication and automated information systems security guidance to the departments and agencies of the government.

(3) Submit annually to the Steering Group an evaluation of the status of national telecommunications and automated information systems security with respect to established objectives and priorities.

(4) Identify systems which handle sensitive, non-government information, the loss and exploitation of which could adversely affect the national security interest, for the purpose of encouraging, advising and, where appropriate, assisting the private sector in applying security measures.

(5) Approve the release of sensitive systems technical security material, information, and techniques to foreign governments or international organizations with the concurrence of the Director of Central Intelligence for those activities which he manages.

(6) Establish and maintain a national system for promulgating the operating policies, directives, and guidance which may be issued pursuant to this Directive.

(7) Establish permanent and temporary subcommittees as necessary to discharge its responsibilities.

(8) Make recommendations to the Steering Group on Committee membership and establish criteria and procedures for permanent observers from other departments or agencies affected by specific matters under deliberation, who may attend meetings upon invitation of the Chairman.

(9) Interact with the National Communications System Committee of Principals established by Executive Order

12472 to ensure the coordinated execution of assigned responsibilities.

c. The Committee shall have two subcommittees, one focusing on telecommunications security and one focusing on automated information systems security. The two subcommittees shall interact closely and any recommendations concerning implementation of protective measures shall combine and coordinate both areas where appropriate, while considering any differences in the level of maturity of the technologies to support such implementation. However, the level of maturity of one technology shall not impede implementation in other areas which are deemed feasible and important.

d. The Committee shall have a permanent secretariat composed of personnel of the National Security Agency and such other personnel from departments and agencies represented on the Committee as are requested by the Chairman. The National Security Agency shall provide facilities and support as required. Other departments and agencies shall provide facilities and support as requested by the Chairman.

6. The Executive Agent of the Government for Telecommunications and Information Systems Security. The Secretary of Defense is the Executive Agent of the Government for Communications Security under authority of Executive Order 12333. By authority of this Directive he shall serve an expanded role as Executive Agent of the Government for Telecommunications and Automated Information Systems Security and shall be responsible for implementing, under his signature, the policies developed by the NTISSC. In this capacity he shall act in accordance with policies and procedures established by the Steering Group and the NTISSC to:

a. Ensure the development, in conjunction with NTISSC member departments and agencies, of plans and programs to fulfill the objectives of this Directive, including the development of necessary security architectures.

b. Procure for and provide to departments and agencies of the government and, where appropriate, to private institutions (including government contractors) and foreign governments, technical security material, other technical assistance, and other related services of common concern, as required to accomplish the objectives of this Directive.

c. Approve and provide minimum security standards and doctrine, consistent with provisions of the Directive.

d. Conduct, approve, or endorse research and development of techniques and equipment for telecommunications and automated information systems security for national security information.

e. Operate, or coordinate the efforts of, government technical centers related to telecommunications and automated information systems security.

f. Review and assess for the Steering Group the proposed telecommunications systems security programs and budgets for the departments and agencies of the government for each fiscal year and recommend alternatives, where appropriate. The views of all affected departments and agencies shall be fully expressed to the Steering Group.

g. Review for the Steering Group the aggregated automated information systems security program and budget recommendations of the departments and agencies of the US Government for each fiscal year.

7. The National Manager for Telecommunications Security and Automated Information Systems Security. The Director, National Security Agency is designated the National Manager for Telecommunications and Automated Information Systems Security and is responsible to the Secretary of Defense as Executive Agent for carrying out the foregoing responsibilities. In fulfilling these responsibilities the National Manager shall have authority in the name of the Executive Agent to:

a. Examine government telecommunications systems and automated information systems and evaluate their vulnerability to hostile interception and exploitation. Any such activities, including those involving monitoring of official telecommunications, shall be conducted in strict compliance with law, Executive Orders and applicable Presidential Directives. No monitoring shall be performed without advising the heads of the agencies, departments, or services concerned.

b. Act as the government focal point for cryptography, telecommunications systems security, and automated information systems security.

c. Conduct, approve, or endorse research and development of techniques and equipment for telecommunications and automated information systems security for national security information.

d. Review and approve all standards, techniques, systems and equipments for telecommunications and automated information systems security.

e. Conduct foreign communications security liaison, including agreements with foreign governments and with international and private organizations for telecommunications and automated information systems security, except for those foreign intelligence relationships conducted for intelligence purposes by the Director of Central Intelligence. Agreements shall be coordinated with affected departments and agencies.

f. Operate such printing and fabrication facilities as may be required to perform critical functions related to the provision of cryptographic and other technical security material or services.

g. Assess the overall security posture and disseminate information on hostile threats to telecommunications and automated information systems security.

h. Operate a central technical center to evaluate and certify the security of telecommunications systems and automated information systems.

i. Prescribe the minimum standards, methods and procedures for protecting cryptographic and other sensitive technical security material, techniques, and information.

j. Review and assess annually the telecommunications systems security programs and budgets of the departments and agencies of the government, and recommend alternatives, where appropriate, for the Executive Agent and the Steering Group.

k. Review annually the aggregated automated information systems security program and budget recommendations of the departments and agencies of the US Government for the Executive Agent and the Steering Group.

l. Request from the heads of departments and agencies such information and technical support as may be needed to discharge the responsibilities assigned herein.

m. Enter into agreements for the procurement of technical security material and other equipment, and their provision to government agencies and, where appropriate, to private organizations, including government contractors, and foreign governments.

8. The Heads of Federal Departments and Agencies shall:

a. Be responsible for achieving and maintaining a secure posture for telecommunications and automated information systems within their departments or agencies.

b. Ensure that the policies, standards and doctrines issued pursuant to this Directive are implemented within their departments or agencies.

c. Provide to the Systems Security Steering Group, the NTISSC, Executive Agent, and the National Manager, as appropriate, such information as may be required to discharge responsibilities assigned herein, consistent with relevant law, Executive Order, and Presidential Directives.

9. Additional Responsibilities.

a. The Secretary of Commerce, through the Director, National Bureau of Standards, shall issue for public use such Federal Information Processing Standards for the security of information in automated information systems as the Steering Group may approve. The Manager, National Communications System, through the Administrator, General Services Administration, shall develop and issue for public use such Federal Telecommunications Standards for the security of information in telecommunications systems as the National Manager may approve. Such standards, while legally applicable only to Federal Departments and Agencies, shall be structured to facilitate their adoption as voluntary American National Standards as a means of encouraging their use by the private sector.

b. The Director, Office of Management and Budget, shall:

(1) Specify data to be provided during the annual budget review by the departments and agencies on programs and budgets relating to telecommunications systems security and automated information systems security of the departments and agencies of the government.

(2) Consolidate and provide such data to the National Manager via the Executive Agent.

(3) Review for consistency with this Directive, and amend as appropriate, OMB Circular A-71 (Transmittal Memorandum No. 1), OMB Circular A-76, as amended, and other OMB policies and regulations which may pertain to the subject matter herein.

10. Nothing in this Directive:

a. Alters the existing authorities of the Director of Central Intelligence, including his responsibility to act as Executive Agent of the Government for technical security countermeasures (TSCM).

b. Provides the NTISSC, the Executive Agent, or the National Manager authority to examine the facilities of other departments and agencies without approval of the head of such department or agency, nor to request or collect information concerning their operation for any purpose not provided for herein.

c. Amends or contravenes the provisions of existing law, Executive Orders, or Presidential Directives which pertain to the privacy aspects or financial management of automated information systems or to the administrative requirements for safeguarding such resources against fraud, abuse, and waste.

d. Is intended to establish additional review processes for the procurement of automated information processing systems.

11. For the purposes of this Directive, the following terms shall have the meanings indicated:

a. Telecommunications means the preparation, transmission, communication or related processing of information by electrical, electromagnetic, electromechnical, or electro-optical means.

b. Automated Information Systems means systems which create, prepare, or manipulate information in electronic form for purposes other than telecommunication, and includes computers, word processing systems, other electronic information handling systems, and associated equipment.

c. Telecommunications and Automated Information Systems Security means protection afforded to telecommunications and automated information systems, in order to prevent exploitation through interception, unauthorized electronic access, or related technical intelligence threats, and to ensure authenticity. Such protection results from the application of security measures (including cryptosecurity, transmission security, emission security, and computer security) to systems which generate, store, process, transfer, or communicate information of use to an adversary, and also includes the physical protection of sensitive technical security material and sensitive technical security information.

d. Technical security material means equipment, components, devices, and associated documentation or other media which pertain to cryptography, or to the securing of telecommunications and automated information systems.

12. The functions of the Interagency Group for Telecommunications Protection and the National Communications Security Committee (NCSC) as established under PD-24 are subsumed by the Systems Security Steering Group and the NTISSC, respectively. The policies established under the authority of the Interagency Group or the NCSC, which have not been superseded by this Directive, shall remain in effect until modified or rescinded by the Steering Group or the NTISSC, respectively.

13. Except for ongoing telecommunications protection activities mandated by and pursuant to PD/NSC-24, that Directive is hereby superseded and cancelled.

Next 6 Page(s) In Document Denied

DIRECTOR OF CENTRAL INTELLIGENCE
Security Committee

Two changes to the minutes should be noted to avoid confusion:

1. The CIA Technical Center mentioned in Paragraph 7 is the Technology Transfer Assessment Center.

2. After the meeting, a change had to be made in the October meeting because of room availability problems. The meeting is
STAT now scheduled for [redacted] on 30 October vice 23 October. The time is still 0930.

STAT [redacted]

CONFIDENTIAL

DIRECTOR OF CENTRAL INTELLIGENCE
SECURITY COMMITTEE
COMPUTER SECURITY SUBCOMMITTEE

2 October 1984
DCISEC-CSS-M166

1. The One Hundred and Sixty-sixth meeting of the Computer
25X1 Security Subcommittee was held on 11 September 1984 at the
25X1 McLean, VA. The following people attended:

25X1 DIA, Chairman
Mr. Dave Jones, Dept. of Energy
Mr. Robert Graytock, Dept. of Justice
Mr. Bill Meehan, FBI
Mrs. Karen Deneroff, Dept. of State
25X1 NSA
Ms. Martha Tofferi, USAF
Mr. Lynn Culkowski, USAF
25X1 SECOM

25X1 2. of the Information Systems Security Staff,
State Department, was introduced as the new permanent representative
25X1 to the Subcommittee; the previous representative, will serve as the alternate. It was proposed that the membership list be revised in view of the recent changes in representation.

ACTION: The Executive Secretary prepare and distribute an updated list of the Subcommittee members.

3. The Chairman referenced a 27 February 1984 letter from the SECOM Chairman, copy attached, requesting the Subcommittee to provide a report on the security status of personal computers as regards the need for a Community security policy.

25X1

ACTION: The Chairman requested that the Subcommittee members provide, to the Executive Secretary before the next meeting, any regulations or directives their respective Agencies may have on personal computers.

25X1

CL BY

DECL OADR

CONFIDENTIAL

4. The Chairman gave an update on the I.C. Compusec Project
25X1 under the contract to [redacted] The overall effort has been somewhat slowed by the inability of the I.C. Staff to get funds to support the actions being proposed by the Project.

a. A Technology Working Group has been formed, chaired
25X1 by [redacted]

25X1 b. It is believed that [redacted] will reconvene his Safeguards Working Group this fall. There was a concern that the intent might be to issue the "Safeguards" document as a replacement for the present Manual associated with DCID 1/16. Discussion of this topic concluded the Subcommittee should prepare its position on that possibility, now.

5. The Chairman also introduced a letter which was signed by the DCI (Serial NFIB-9.1/53, dated 15 August 1984). It was addressed to the NFIB members and requested they take necessary actions to retain or return unto themselves the accreditation of SCI automated handling systems. The premise made is that this authority has been delegated, inconsistent with the provision of DCID 1/16. NFIB members are to respond in sixty days on steps being taken to rectify this situation. The DCI makes an offer to assist as appropriate in NFIB budgetary support if the lack of sufficient accreditation resources is the cause for the present situation. (A copy of the letter, which is classified, was distributed to the members present.)

The Air Force member was aware of the letter and had action to prepare the requested response. No one seemed to know the background on what precipated the DCI letter; nor was anyone aware of any coordination or staffing of it prior to transmittal. There was some discussion that the latest revision of DCID 1/16 which replaced the "NFIB Member" with "SOIC" may have diffused the authority intended.

ACTION: Executive Secretary should place this item on the agenda for the October meeting; members should be prepared to report on how their agencies responded.

6. The Chairman reported that there had been a flurry of activity in early August on the draft National Security Decision Directive (NSDD-xx) which proposes to make the Secretary of Defense Executive Agent for the Government for Computer Security along with his current role for COMSEC. The Chairman described the proposed organizational structure, including the Steering Group at the Cabinet level, the National Telecommunications and Information Systems Security Committee (NTISSC), and the National Manager (DIRNSA). He surmised that the major objections were over the National Manager's "control" of the computer security budget for the government, foreign interface, and monitoring operations. He stated he understood it was in for the President's signature.

7. The Chairman reported that, at this time, there were no funds for FY85 for the Subcommittee to carry out any tasks. The Navy member was not present, but it was assumed that there was continuing support of their project to collect and screen intelligence reports for computer security implications and to develop a methodology for assessing these reports. The Air Force member reported that he would be attending an R&D meeting at ESD, Hanscom Field, on 25 - 27 September, and asked the members to let him know if there were any efforts he should propose the Air Force should consider in support of the Intelligence Community's computer security objectives. The NSA member mentioned the need to address the hardware subversion issue. The Chairman agreed to get the CIA Technical Center to brief the Subcommittee on their work.

ACTION: Chairman arrange for CIA Technical Center to brief the Subcommittee.

8. The NSA member reported that LtCol J. Craig, of the DoD Computer Security Center, would be presenting the Center's Threat Briefing to the SECOM at their September meeting. The Center is also available to provide this briefing to any of the NFIB principals who may not already have heard it.

9. The NSA member mentioned that the DoD Computer Security Center had both a new Director and Deputy Director since the last meeting. The Director is Dr. Robert Brotzman and the Deputy is Col Joseph Greene, Jr, USAF, formerly with the WIS PMO.

10. There being no further business, the Chairman set the time of the next Subcommittee meeting for 23 October 1984, at
25X1 0930, at the [redacted] and adjourned this meeting.

25X1 [redacted]
for the Executive Secretary

Attachment:

SECOM-D-044, dated 27 Feb 84.

DIRECTOR OF CENTRAL INTELLIGENCE

Security Committee

SECOM-D-044

27 February 1984

STAT MEMORANDUM FOR: [redacted] Chairman
SECOM Computer Security Subcommittee

STAT FROM: [redacted]
Chairman

SUBJECT: Policy on Personal Computers in the Intelligence Community

1. As we discussed recently, I have been asked by the Intelligence Community Staff policy officer whether there is a Community security policy concerning "personal computers". At that time, you provided me some information on possible areas of vulnerability, but advised that policy on personal computers is currently made by individual agencies.

2. I feel constrained to provide as definitive an answer as possible to this query. Therefore, I request that you place this matter on the agenda of the Computer Security Subcommittee, with the objective of providing a report on the security status of personal computers. In addition to the matter of the distinction between personally-owned computers and the class of mini-computers called personal computers, the report should address the following:

a. Do all member agencies have written regulations on the use of personally-owned or personal-sized computers? What are the significant similarities or differences in the guidance?

b. Does the Subcommittee feel that the proliferation of these devices, the lack of controls, or the technical weaknesses of these systems present a threat significant enough to address as a special category of computer security? If so, please state in some detail the aspects which are particularly hazardous.

c. What are the potential security vulnerabilities inherent in the use of personal computers?

ILLEGIB [redacted]

d. Based on the above, does the Subcommittee feel the need for a Community policy on "personal computers" to provide uniform protection for the intelligence stored or procesed thereon?

3. Your assistance in the matter is, as always, greatly appreciated.

STAT